U.S. Department of Justice

United States Attorney
Southern District of New York

The Silvio J. Mollo Building
One Saint Andrew's Plaza
New York, New York 10007

August 12, 2020

By ECF
The Honorable Paul A. Crotty
United States District Judge
Southern District of New York
500 Pearl Street, Courtroom 14C
New York, New York 10007

Re: *United States v. Joshua Adam Schulte*, S3 17 Cr. 548 (PAC)

Dear Judge Crotty:

We write in response to the defendant's July 28, 2020 letter renewing his request for full mirror images of the Central Intelligence Agency's ESXi and NetApp servers. To be clear, the defendant is, in effect, requesting full access to DEVLAN—a breathtaking amount of highly classified data that has no relevance to the issues at trial or the opinions offered by the Government's experts. Indeed, a full image of the NetApp server alone is enormous and includes, among other things, numerous daily backups of DEVLAN's components and final copies of cyber tools that were never disclosed by WikiLeaks. In support of this vast request, which the Court has repeatedly denied, the defendant mischaracterizes the record and otherwise fails to identify any specific aspect of forensic discovery that was deficient. The defendant's request should be denied once again.

By way of background, on July 22, 2019, the Court issued an order granting, in part, the Government's motion pursuant to Section 4 of the Classified Information Procedures Act ("CIPA"). (Dkt. 124). As relevant here, the Court reviewed and approved the Government's methodology for producing forensic discovery in this case, which included, among many other things, producing all of the log files (*i.e.*, files showing user activities on the server) from the ESXi server and the relevant backups (*i.e.*, the March 3, 2016 backup files that the defendant stole and provided to WikiLeaks) from the NetApp server. (*Id.* at 9-13). In so ruling, the Court explained:

> Of course, the Court is mindful of the immense size of the full universe of forensic data and of the serious national security concerns inherent to producing the totality of Schulte's requests [for forensic images of all of DEVLAN]. The Government put in a great deal of planning and effort in collecting, reviewing, and producing what might be an unprecedented volume of classified discovery to Schulte. Complete forensic copies of . . . DEVLAN would contain a tremendous amount of classified information. . . . Schulte has been accused of leaking information he obtained from his employment at the CIA both before he was arrested and from his cell at MCC after his arrest. Granting him unfettered access to . . . DEVLAN would gut the entire rationale behind CIPA.

(Dkt. 124 at 11-12). The Court also left open the possibility of ordering the production of additional forensic material "if Schulte submits a more tailored request and provides good reason for further forensic discovery." (*Id.* at 12). When the defendant made such requests, as described below, the Government responded, producing substantial additional forensic evidence.

Nonetheless, the defendant persists in making a broad—rather than tailored—and unjustified request for unlimited access to the ESXi and NetApp servers. The defendant's request is hardly "more focused" than his request for a complete forensic image of DEVLAN. (Ltr. at 1). As several witnesses testified, the NetApp is a storage server used to maintain, among other things, daily backup files for DEVLAN's components, home directories for DEVLAN users, and the final copies of cyber tools. (Leedom Tr. 939-40, 943-44, 947-50; Weber Tr. 224-27; David Tr. 787-92). Thus, the NetApp's mirror image would contain a massive amount of data that would take months, if not longer, to review. The overwhelming majority of this data has nothing to do with this case. For example, daily DEVLAN backup files from before or after the date of the theft would provide no insight into who stole the backup files that were disclosed by WikiLeaks (and which were produced in discovery to the defendant). Similarly, the ESXi server was used, and thus would contain data related to, classified programs and projects that were entirely unrelated to the theft of classified information at issue in this case. (Weber Tr. 218-20; 238-40). As the Court has already found, providing irrelevant but highly classified information to the defendant—who is accused of leaking classified information from prison after being charged with leaking classified information from the CIA—would "gut the entire rationale beyond CIPA." (Dkt. 124, at 12).

In attempting to justify his renewed request, the defendant continues to mischaracterize the record and distort the facts. For example, (i) the defendant cites his earlier claim that he was not afforded access to the March 3, 2016 backup files from the NetApp server (Dkt. 328, at 9), when in fact those backup files were produced on December 10, 2018 and then again on a standalone computer in November 2019 (Dkt. 329, at 17-18); (ii) the defendant references his previous argument that he had "no access whatsoever to [the] unallocated space [from the ESXi server]" (Dkt. 328, at 11), but on December 10, 2018 and June 14, 2019, the Government produced all of the portions of unallocated space for the ESXi server about which Patrick Leedom, one of the Government's forensic experts, testified (Dkt. 329, at 19); and (iii) the defendant claimed that the log files from the ESXi server produced by the Government in discovery were "demonstrably damaged" as a "result of prior forensic examination" (Dkt. 331-1, at 4), but on June 14, 2019, in response to the defendant's request, the Government produced unmodified copies in their original format of both log files and unallocated space from the ESXi server (Dkt. 332, at 1).

The defendant does not address these factual inaccuracies in his July 28, 2020 letter. Instead, he focuses on a single line of Mr. Leedom's cross-examination testimony. In particular, after being asked a few questions about his access to mirror images to CIA computer systems, Mr. Leedom responded "correct" when asked by defense counsel whether his access to those images "very much informed" his expert opinion. (Tr. 1187). From this, the defendant claims that Mr. Leedom "acknowledged [the] materiality" of the servers to his expert opinions. This is wrong. As an initial matter, Mr. Leedom's testimony spanned nearly 300 transcript pages (Tr. 908-1201) and included a 191-page expert report (GX 1703). The defendant has cherry-picked one answer to inappropriately suggest that Mr. Leedom based his opinions on data not provided to the defense.

This mischaracterizes the testimony and the Government's disclosure obligations, which the Government has complied with by providing the defendant with the facts and data upon which Mr. Leedom based his opinions. *See* Fed. R. Evid. 702 ("A witness who is qualified as an expert . . . may testify in the form of an opinion or otherwise if . . . the testimony is based on sufficient facts or data . . . ."); *see also* Fed. R. Evid. 703; Fed. R. Crim. P. 16(a)(1)(G). In that respect, as Mr. Leedom's lengthy description of his expert analysis makes clear, none of the opinions to which Mr. Leedom testified relied on any information from the images of the ESXi and NetApp Servers beyond what was produced to the defense. Rather, Mr. Leedom testified in painstaking detail about specific forensic artifacts taken from those servers (all of which were produced to the defense) and explained how each of those artifacts supported his opinions. Indeed, starting in July 2019, the Government began to identify to the defense those specific forensic artifacts underlying Mr. Leedom's opinions. The parties discussed those forensic artifacts extensively during CIPA proceedings in November and December 2019, well in advance of trial. The Government also produced a detailed expert notice to the defense on October 18, 2019 (and that notice stated that Mr. Leedom's opinions were based on the forensic materials produced in discovery to the defendant), and began producing drafts of Mr. Leedom's trial presentation weeks before trial. No more was required under the Federal Rules of Evidence.

The defendant's related suggestion that the Government misled the Court in its CIPA Section 4 brief is baseless. (Ltr. at 1-2). The Government was, of course, clear in that brief that the Government had full access to CIA computer systems and asked for permission to withhold portions of those systems from the defense. The Government's rationale was that the key issues in this case were who had access to the classified information on DEVLAN, stole that information, and then provided it to WikiLeaks, and that the forensic files being produced in discovery were sufficient to address those issues. That is precisely the information that Mr. Leedom relied on in forming his expert opinion and testifying at trial.[1] Nor is this case—in which Mr. Leedom, who participated in the underlying investigation and thus had access to DEVLAN systems at the CIA facility in which they were stored—anything like *United States v. Shrake*, 515 F.3d 743, 746 (7th Cir. 2008) upon which the defendant relies. *Shrake* was a child pornography case in which the Government had retained a private expert and provided that expert with a mirror image of a computer hard disk outside of government facilities, in violation of the restrictions on such material imposed by the Adam Walsh Child Protection and Safety Act, while denying the defense expert the same production.

Finally, the defendant contends that the Court should grant his request because, according to him, the Government's "evidence is not nearly as strong as it pretends" and that he may be able to prove his alleged innocence if given full access to these servers. (Ltr. at 2). Such a speculative request has no merit—the defendant does not have a "constitutional right to conduct his own search of the [Government's] files to argue relevance." *Pennsylvania v. Ritchie,* 480 U.S. 39,

[1] The defendant is also wrong that the issue that arose with Michael at trial supports revisiting the Section 4 ruling. (Ltr. at 2 n.2). As the Government made clear in its opposition to the defendant's mistrial motion, the defendant possessed all of the relevant forensic information relating to the CIA's decision to place Michael on administrative leave for months or longer before trial, and the Government did not suppress material information, although it acknowledged that it should have provided information on Michael's administrative leave status sooner. (Dkt. 329, at 14-22).

59 (1987). Moreover, the defendant's position, which he offers without explanation, is belied by the extensive trial record in this case, which the Government reviewed in its opposition to the defendant's Rule 29 motion (Dkt. 410, at 2-24). The defendant had an opportunity to contest the Government's characterization of the trial evidence, but he "decided not to file a reply." (Dkt. 415). Regardless, if the defendant believes that the Government's evidence "is not nearly as strong as it pretends," the best way to test the Government's evidence is to schedule and hold the retrial as quickly as possible. In that respect, as the Government has noted, the Government anticipates that the retrial will be substantially shorter than the first trial because the Government intends to call fewer witnesses and scale back its case. The defendant's current request for vast forensic discovery would substantially delay scheduling the retrial, in that granting his request would delay this case for months or, likely, much longer. There is no basis to do so on the current record. The defendant's request should be denied.

Respectfully submitted,

AUDREY STRAUSS
Acting United States Attorney

by: /s/
David W. Denton, Jr. / Sidhardha Kamaraju /
Matthew Laroche
Assistant United States Attorneys
(212) 637-2744 / 6523 / 2420

cc: Defense Counsel (by ECF)